Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 04, April -2018

AUTHENTICATION VIA SECRET QUESTIONS AND SPACIO-LOCATION WITH SMARTPHONE AND APP USING HYBRID ENCRYPTION PASSWORD TECHNIQUE

Ms.ShitalM.Gujarathi#1 Prof. Vikas Nandgaonkar[2]

[1]Department of Computer Engineering, NMIET, Pune,India
2.Department of Computer Engineering, NMIET,Pune,India

Abstract —*Atpresent with growing popularity of on the internet purchasing Debit or Credit card fraud. Personalized data securities are main considerations for all. Several worldwide network application supply secondary verification techniques i.e., leading confidential query (or retrieve forgot password queries), to reboot the account password once a user's login fails. Nowadays prevalence of intelligent phones has authorized us latest possibility to monitor and recognize the personal information gather by intelligent mobile phone detector and apps can guide to develop and modified the confidential question not including having abusing the customers confidentiality issues. We current a new login technique exactly where customers supply username, secrete location and secret keyword to login. We also use Confidential-Queries based on typically verification method, known as Confidential-Query that generates a set of confidential questions on standard of people sensible mobile phone utilization. If some of purpose user forgot password or mistype password then user can't accessibility his/her account. To get the accessibility of account user have to reply the security question. In current method User supply password recovery electronic mail id, mobile number at the time of registration. System user can reset his/her password by electronic mail, mobile. Third party authentication technique generates bunch of confidential queries according to the information of end users every day action. We evaluated the dependability and protection by making use of accurate true/false variety secret questions. To provide the additional security to secret location and secret keyword using hybrid encryption technique which is combination of AES blowfish algorithm. The best objective of the examination provided in this paper is to develop both AES as well as Blowfish to be decreased power, actual-time, superior bandwidth, reputable and also incredibly secure cryptography formula. Evaluation of AES and blowfish algorithm is tough to make sure thathacker does not possible to hack the system.*

Keywords- *smart phone sensor, Geo-location, AES algorithm, blowfish algorithm, Annotation password,hyprid encryption password technique, KNN algorithm.*

I.INTRODUCTION

Android Security is a technological innovation that supplies accessibility to details and calculating sources that accessible the network from anyplace. There is a need to have to safe the information stored on server. The major purpose of style of encoding algorithm need to be safety towards unwanted attacks.Even so, for all Android apps.Functionality and value of implementation are main considerations. The protection and efficiency of encryption algorithms have to be stabled. Security algorithms used in this paper, to evaluate the performance level of every algorithm.
Additional Verification can be classified in 2 kinds.
1) User can login the system by providing answer to the protected question when he/she forgot the password.
2) If user can get access to extremely confidential data or information like banking by providing solution to the protected inquiry.

Password recovery inquiries are generally made use by a great deal of internet Solutions as the additional verification strategy for resetting the forgot account password by the user. It also generate the user account on normally utilized internet sites like Gmail, yahoo etc. Customer need to choose questions from established list of the Questions. All these are empty fillings. Customer can reset his account password by providing theappropriate solution to the safety and confidential Question. For the easily memorizing the answers most of the confidential questions are empty-fillings which are developed based on the personalized background of the user.(e.g., What is of your pet's name?). So the investigation has exposed that this type of empty-filling questions designed on the basis of user's personalized information may possibly lead to poor security and dependability as answers of this type of Questions can be guessed by the using of social networking websites. The prevalence of intelligent mobile application has presented a source of the users personalized information which is relevant to the understanding of his quick-phrase background, i.e., the information gathered by the intelligent mobile application.
Sensors and apps can be utilized for generating the confidential Questions. Brief - phrase personalized story typically inside of particular month) can be utilized. Very less probably to exposed to know the personalize history to the stranger or familiarity, because the quick modifications of an event that a person has skilled inside of a quick phrase will improve the resilience to guess attacks. This implies enhanced security forSuch confidential questions.

Propose system current a confidential-Question based authorized method, with the benefit of the data of intelligent mobile application without having violating the user privacy. In this Authentication technique questions are Accurate/false for easier remembrance of user. Hybrid Security Algorithm is symmetrical block cipher algorithm, It is a mix of two identified algorithms (Blowfish AES 128).

Hybrid Security Algorithm requires the advantages of blowfish algorithm and also Advanced Encryption-Standard (AES) algorithm could make it harder for any kind of opponent to aim to decrypt the cipher message.

II.LITERATUREREVIEW

1.Reference paper [1] author says in his research when user login fails, to reset the account password numerous world wide applications provide the secondary verification techniques. Even so, the answers to numerous kind of confidential queries can be very easily guessed by an familiarity or exposed to a outsider that has accessibility to public on the web resources (e.g., on the internet social networks); Nodaway's superiority of smart phones has provide us new possibility to observe and realize how the individual information gathered by smart-phone detectors and apps can help generate personal confidential questionswithout affecting the end users privacy matter. This paper used user event extraction method in which smart phone detector and app which capture various event related to users daily activities, confidential QA selected list of detector and app extract the user activity and data standard encryption use for security to protect information send between browser and server including password encryption technique which encrypt plain text to cipher text and uses 16 round of structure and block size is 64 bit. It uses same key to encrypt anddecrypt the message so both sender and receiver must know and use the same private key.
Advantage:
Encrypt message using DES algorithm
Disadvantage:
System does not provide that much any security to user data

2. Paper [2] professor says in his studies nearly all internet sites that keep user-certain accounts use passwords to confirm that a user associate degree try to accessibility an account is, in reality, the account holder. Even so, sites need to even now be ready to establish users United Nations Companycan'tsupply their appropriate parole, as passwords could be lost, forgotten, or stolen. For the duration of this situation, users would need a variety of secondary authentication to show that they're United Nations agency they assert they're and regain account accessibility.
Method:
Knowledge Based Verification Technique.
Transitive Verification Technique.
Method Description:
1. Transitive Secondary Verification Technique.
Knowledge-based verification systems are well-known wit social media and other access granters because they are relatively simple to execute and it is not carrying on outside infrastructure, such as other systems or specific hardware.
2. Transitive Verification Technique.
Transitive verification systems provide the information about validating users to a system user that's better arrange to authenticate users than the website.
Advantages:
Easy to use
Disadvantages:
User need to pay for secondary authentication (email/SMS).

3. Paper [3] mentioned the Sensor network technology has obtained growing not too long ago. Sensing component network technologies is to sense Associate in Nursing object or environmental information and gather, analyses and technique essential information so as to predict and forestall Disasters. Sensing component network technological innovation consists of wireless communication and as a outcome of the reduced computing capability and limited energy supplies, security chance will improve. Throughout this review, authentication protocol is meant to spot etch sensors by exploitation HIGHT creating rule inside ofthe excellent cellphone setting. And consequently the authentication record inside of the authentication server is inspected to provide solely conventional sensing component information to Disaster support users throughout this planned authentication protocol.
Method:
HIGHT algorithm is used for data encryption.
Method Description:
To protect Beacon sensor authentication information generated in Disaster areas and Disaster service data, the 64bits block ciphering algorithm, HIGHT (TTAS.KO-12.0040) is employed in this study. HIGHT was designed in consideration of low power computing environment, using 6bits plain blocks and 128bits key as input to output 64bits cryptogram block.
Advantages:
Block size 64-bit and key size 128-bit

Same algorithm used for other application for data encryption
Disadvantages:
Complex system
4. Paper [4] presents an identity verification mechanism exploitation movement sensing component of excellentmobile phone. The user wants to carry signature by moving his mobile phone, the movement pattern is detected exploitation measuring instrument of the excellent mobile phone. Wave received utilized the suggestions of signal matching for identification mechanism. Final results depict that reputable user will be identified using a bound degree of error threshold.
Method:
Cross Correlation of Signature
Method Description:
Accelerometer of the Smartphone provides data obtained for all three axes separately. Therefore, data of each axis is to be matched with its corresponding axis in the template data. The data for each axis can be plotted as function of time.
Advantages:
This technique is more secure than traditional username
Password and similar kind of methods.
Disadvantages:
System is not reliable for daily usage use.

PROBLEMSTATMENT

To keep in mind the difficult password is really inconvenient occupation, because it's a combination of alphanumeric and particular symbol. If some of purpose user forgot password or mistype password then user can't accessibility his/her account. To get the accessibility of account user have to reply the security question. Security question and answer are recorded at the time user registration. Right after lengthy time it's challenging to remember the security answer. At the identical time for hacker or malicious user it's easy to guise the password. To keep away from these difficulties we propose system that can more than all thread from current technique. Encoding algorithm would not be of considerably use if it is extremelysignificantly safe but slow in efficiency. Blowfish algorithm is quickest as compare to other algorithms but it has significantly less security than the AES. To conquer these weaknesses, we use combinational model implementation which is AES with Blowfish algorithm.

III. EXISTING SYSTEM

Existing authentication methods depend mainly on blank-filling questions, because the lightweight questions are subject to the random guessing attacks, e.g., a 50% success rate for an attacker given a true-false question.

In existing system User provide password recovery email id, mobile number at the time of registration. System user can reset his/her password by email, mobile. Third party authentication system generates set of secret questions created based on the data of user's daily activity and short-term smart phone usage. Daily activity contain call logs, user visited location.

In Existing Symmetric techniques like DES, IDEA, Blowfish, RC4, RC5, RC2, Triple DES, and AES. DES algorithm use feistel system, the key size is 56bit. Due to small key size DES is insecure and has weaknesses. Triple DES which is an improvement to DES, the original DES algorithm was applied thrice to enhance the protection. But it was found to be very slow. Blowfish algorithm runs earlier than other symmetric algorithms. The AES is recommended symmetrical based encryption standard by NIST.AES algorithm is the best encryption algorithm.

V.DISADVANTAGE OF EXISTING SYSTEM

- Need to remember combination of alphanumeric and special symbol string called as password.
- Change in spelling cause wrong answer. Need to remember exact spelling.
- System does not provide any security to user data.

VI.PROPOSE SYSTEM

We design a user authentication technique where user register into technique by delivering identify, mobile number, electronic mail id. User login with user identify and secret location with secret keyword. If user forgets the secret location or secret keyword then user will solution set of confidential questions designed primarily based on information of user's everyday action and quick-phrase intelligent mobile phone utilization.
Characteristic variety will be utilized to decide on question type by information collected from mobile sensors. We evaluated the dependability and security by utilizing accurate/false type secret questions. These questions are straightforward to answer and no need to remember due to the fact these are on primarily based on user personalized

daily life and events. Due to this application security will be improve simply because only user knew the events and issues he/she did recently. To provide the additional security to secret location and secret keyword will be dual encrypted with AES blowfish algorithm. This new created encrypted info will be used as encryption essential of blowfish algorithm. With the support of blowfish algorithm encrypted keyword yet again get encrypt. If user failed to authenticate himself then present location will be fetched and technique will capture picture of user by utilizing front camera and information will be send to users registered on electronic mail id or mobile number. If users personalized activity information is not accessible for much more than amonth at that time user will be authenticated with its registered electronic mail id and mobile number and if authentication passed successfully then user will obtain a reset password notification on his registered mail Id.

VII.ADVANTAGE OF PROPOSE SYSTEM

- The hybrid encryption technique provide less power, superior bandwidth, actual time and particularly securealgorithms.
- No need to remember password for login.
- No need to remember question answer for long time.
- Terminate part of spelling mistakes.
- Secrete location and secret key word is encrypted by AES and blowfish.
- Propose system provide double security by dual encryption.
- The hybrid of AES and Blowfish algorithm has characteristics of both the algorithms and it makes the algorithm strong against vulnerabilities.
- This hybrid structure of enhanced AES and Blowfish provides more security by increasing the complexity
- It also provides a methodology for obtaining high-speed, efficient and scalable implementation of protocols for authentication and key agreement.

VIII.METHODOLOGIES AND ALGORITHM

1. Hybrid Encryption password technique

Encryption: There are four components to this algorithm:

1. Component 1: This parts consist of Blowfish key which discontinues the collection of sub keys. Particularly, a key of no greater than 448 bits is divided into 4168 bytes. It consist P-array having 18 sub keys of 32-bit and four 32- bit S-boxes include 256 access.
2. Component 2: This parts consist of AES key which used to development of 128 bit just from the essential which will certainly provide 10 partial keys utilized in the first round, 9 major rounds and also one last round.
3.Component 3: From simple message it create the security of 128 bit utilizing blowfish by creating encoding to the initial 64 bit then other 64 bit.
4. Component 4: Get the result of encoded 128 bit which from blowfish two times and use this result as a input simple message to AES algorithm

Decryption:
1. Component that manages the development of the vital utilized in blowfish.
2. Component that manages the development of the vital utilized in AES.
3. Component that manages the decoding utilizing AES128 to the encoded information utilizing blowfish
4. Component that manage the decoding of the informationutilizing blowfish. Component 1 and 2 are equal coincide in decoding component which is not modified in vital generation for both blowfish, AES algorithm. For component 3 and 4 we will certainly begin with component 4 after that component 3.
It generally begins with input key from customer and create blowfish encoding data twice which obtain 128 encoding data. After that AES technique use one time to the 128 bit encoding data which coming output from twice blowfish technique. Initial 128 bit use as key which could obtain higher to 448 bit or 576 bit key in blowfish.After that ultimately we obtained the 128 bit encoded.

2. Haversine algorithm to calculate the distance from target point to origin point

1. R is the radius of earth in meters.
   Lat_O= latitude of origin point, $Long_O$ = longitude of origin point
   Lat_T= latitude of target point, $Long_T$= longitude of target point
2. Difference in latitude = Lat_O-Lat_T Difference in longitude = $Long_O$-$Long_T$
3. Φ =Difference in latitude in radians

Λ =Difference in longitude in radians
O= Lat_O in radians. T= Lat_T in radians.

4. A= sin(Φ/2) * sin(Φ/2) + cos(O) *cos(T)*sin(Λ/2)*sin(Λ/2)
5. B= min(1,sqrt(A))
   Distance = 2*R*B

3. K-nearest neighbors KNN algorithm:

1. Determine parameter K = number of nearest neighbors

2. Calculate the distance between the query-instance and all the training samples

3. Sort the distance and determine nearest neighbors based on the K-th minimum distance

4. Gather the category y of the nearest neighbors

5. Use simple majority of the category of nearest neighbors as the prediction value of the query instance

KNN psudocode

```
Classify (X, Y, x) // X: training data, Y: class labels of X, x: unknown sample for
i=1 to m do
Compute distance d(Xi, x)
End for
Compute set I containing indices for the k smallest distances d(Xi, x). return
majority label for {Yi where i E I}
```

IX.SYSTEM ARCHITECTURE

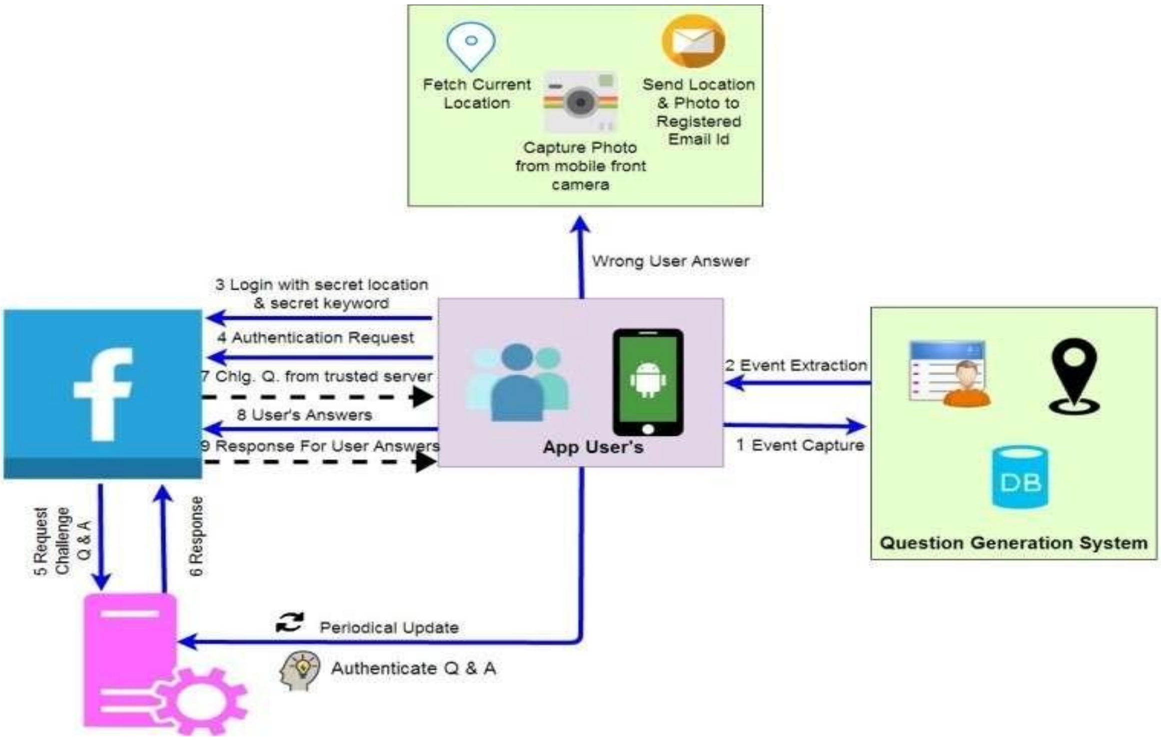
Fetch Current Location
Send Location & Photo to Registered Email Id
Capture Photo from mobile front camera
Wrong User Answer
3 Login with secret location & secret keyword
4 Authentication Request
7 Chlg. Q. from trusted server
8 User's Answers
9 Response For User Answers
App User's
2 Event Extraction
1 Event Capture
DB
Question Generation System
5 Request Challenge Q & A
6 Response
Periodical Update
Authenticate Q & A

FIG1.SYSTEM ARCHITECTURE

Application user performs daily activity. At background user event like location of user, call log history capture and store into database. Event extraction performs on this data. This data periodically updated into server. User will login to system with user name, secret location, and secret keyword. If user forget secret location or secret keyword then user request to reset password on dummy social networking site. This request sends to server. Server sends questions & answer into response.

X.MATHEMATICAL MODEL AND DESIGN

Let S be the Whole system which consists:S= {IP, Pro, OP}
Where,
A. IP is the input of the system. B. Pro is the procedure applied to the system to process the
Given input. C. OP is the output of the system.

A. Input:
IP = {OTP, L, CL, ANS}
Where,
1. OTP-One Time Password

1. L - User Password Location.

2. A- Annotation

3. CL - Call Logs

4. ANS - Answer Submitted by User

B. Process

1. Send OTP on User mobile
2. System verify OTP enter by user
3. Extract the question and answer from user data
4. Periodically update the question and answer on server
5. User ask for reset password on social media
6. Question answer will fetch from server
7. Get the answer from user and match with database answer
8. If answer are correct then select user location and matchlocation using K-nn algorithm and verify location password
9. Then insert Annotation and Encrypt Annotation usingHybrid algorithm and verify with Annotation password
10. If all step are correct then reset password
11. If answer are incorrect then capture photo and send tothe register email id

C. Output:
OP={srp, cp, pe}
srp= successfully reset password,
cp= capture photo,
pe= send photo to register email id

XI.PERFORMANCE MEASURE AND EFFICIENCYCALCULATION

TABLE I
PERFORMANCE MEASURE TABLE OF ENCRYPTION TIME

	Encryption DES	Encryption Blowfish	Encryption Hybrid
10 KB	0.4	0.3	0.3
50 KB	1.4	1.3	1.2
100 KB	2.7	2.6	2.5
200 KB	5.4	5.3	5

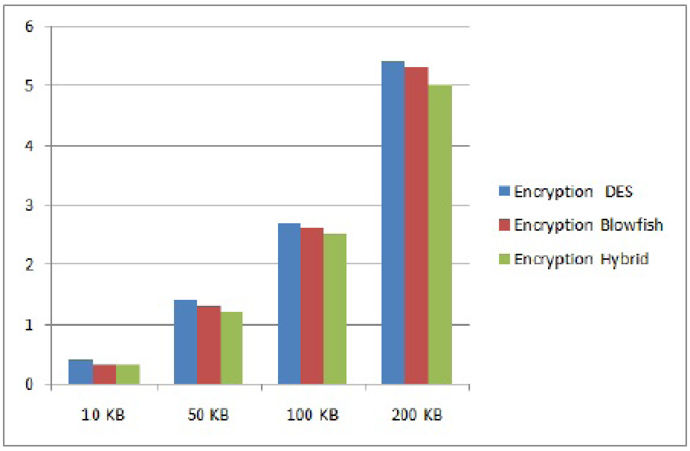

Fig. 2. Performance measure Graph of Encryption Time

TABLE II
PERFORMANCE MEASURE TABLE OF DECRYPTION TIME

	Decryption DES	Decryption Blowfish	Decryption Hybrid
10 KB	0.3	0.3	0.2
50 KB	1.2	1.2	1
100 KB	2.3	2.5	2
200 KB	5	5.2	3.5

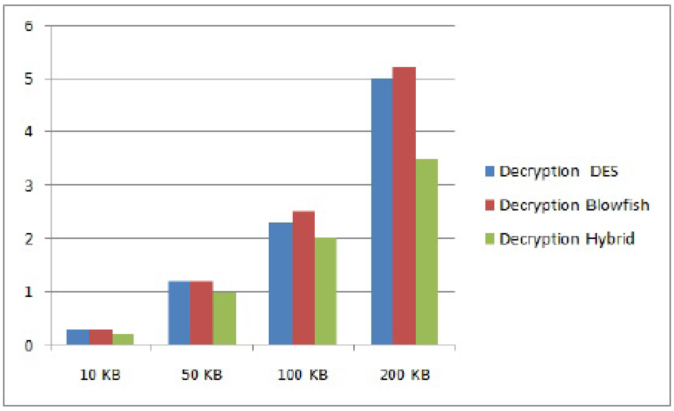

Fig. 3. Performance measure Graph of Decryption Time

XII.CONCLUSION

In propose system user login with user name, secret location and secret keyword. So no need to have to keep in mind password for login. If user fail to remember the secret locationor secret keyword then propose technique ask question to userwhich are basis on users personalized daily life on the basisof quick time period and current activity. Question created onthe basis of information collected by intelligent mobile phonesensor and app. To provide extra security to secret location andsecrete keyword using hybrid encryption password techniquewhich is combination off AES and Blowfish algorithm whichprovide low power, highthroughput ,real time, reliable, fast,technique. Which is extremely secure cryptographic algorithm.Propose technique request confidential queries without affectingthe end users privateness. In propose system user noneed to have to keep in mind question answer for lengthytime period. If user failed to authenticate himself then presentlocation will be fetched and system will capture picture ofuser by utilizing front camera and information will be send tousers registered on electronic mail id or mobile number.

REFERENCES

[1] Peng Zhao, KaiguiBian, Tong Zhao, Xintong Song, Jung-Min Jerry Park,Xiaoming Li, Fan Ye, Wei Yan, Understanding Smartphone Sensor andApp Data for Enhancing the Security of Secret Questions, pp.99, 2016.

[2] R. Reeder and S. Schechter, When the password doesn’t work: Secondaryauthentication for websites, S P., IEEE, vol. 9, no. 2, pp. 4349, March2011.

[3] Jae-Pil Lee, Jae-Gwang Lee, Eun-su Mo, Jun-hyeon Lee, Ki-su Yoon,Jae-KwangLeeDesign of Smartphone based Authentication Protocol forBeacon Detection in Disaster System, IEEE (ICEICT) 2016.

[4] AsadullahLaghari; Waheed-ur-Rehman; Zulfiqar Ali Memon, Biometricauthentication technique using smartphone sensor,13th InternationalBhurban Conference on Applied Sciences and Technology (IBCAST)2016.

[5] Aditi Roy; TziporaHalevi; NasirMemon, An HMM-based multi-sensorapproach for continuous mobile authentication, IEEE Military CommunicationsConference, 2015.

[6] Masao Yamazaki; Dongju Li; Tsuyoshi Isshiki; Hiroaki Kunieda,SIFTbasedalgorithm for fingerprint authentication on smartphone,6th InternationalConference of Information and Communication Technology forEmbedded Systems (IC-ICTES),2015 57 .

[7] SamuliHemminki, PetteriNurmi, SasuTarkoma, Accelerometer-BasedTransportation Mode Detection on Smartphones, 6EIT ICT Labs, theTIVIT IoT SHOK programme and the TIVIT D2I SHOK programme.2013.

[8] N. Roy, H. Wang, and R. R. Choudhury, I am a smartphone and I can tellmy users walking direction, in Proc. ACM MobiSys, 2014, pp.329342.

[9] .H. Kim, J. Tang, and R. Anderson, Social authentication: harder than itlooks, in Financial Cryptography and Data Security. Springer, 2012, pp.115.8.N. Roy, H. Wang, and R. R. Choudhury, I am a smartphone and I can tell my user's walking direction, in Proc. ACM MobiSys, 2014, pp.329–342.